SSL Decryption Certificates

Tech Note

Overview

The Palo Alto Networks security gateway is capable of decrypting outbound SSL connections for the purpose of providing visibility and control of the traffic, without compromising the security or privacy of the traffic. This action is off by default and can be enabled selectively by policy, including source, destination, and URL category. To accomplish this, the Palo Alto device proxies the SSL connection, terminating the connection from the client and re-establishing the SSL connection to the destination server. Traffic in the SSL connection is then identified by application for visibility and control, but re-encrypted to ensure continued privacy and security.

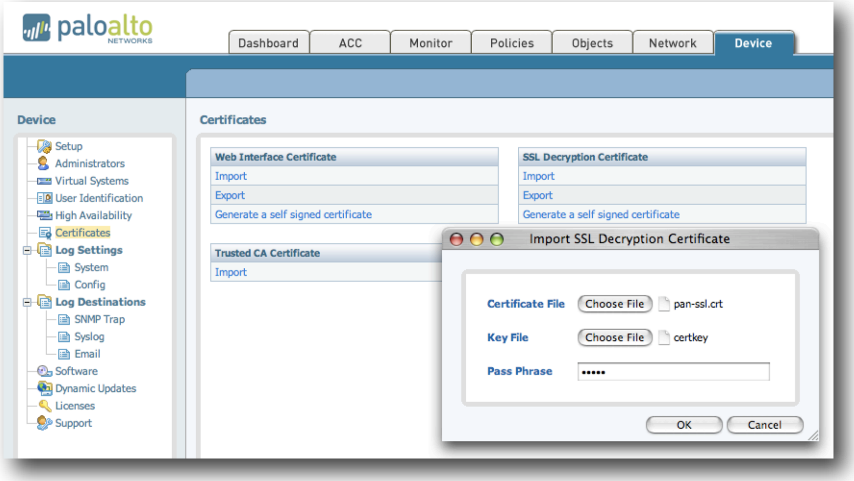
This document is intended to provide an overview of how to manage SSL certificates for the purpose of using the Palo Alto Networks security device for decrypting and inspecting outgoing SSL traffic, as well as loading the public certificate into the users' browser as a trusted root certificate to avoid certificate mis-match warning messages.

Local Certificate Authority

In order to decrypt the SSL sessions, a CA certificate is required. This certificate is used to generate certificates for each SSL destination. By default, a self-signed certificate is used. Because this certificate is not a "Trusted CA", browsers and other applications will give the users a warning indicating that the identity of site they are accessing could not be verified. The browsers can be configured to trust the CA certificate by importing it into the browser. Alternatively, an already trusted CA cert that is used in the enterprise can be installed into the device for use in the SSL decryption process. The following sections will describe common ways to load certificates into the Palo Alto Networks device, how to load trusted CA certificates into a user's browser manually, and how to use Microsoft's Active Directory Group Policy Object tool to automatically load the CA certificate into Windows for use by Internet Explorer.

Using an Enterprise Certificate

A certificate that is already configured as a "Trusted CA" can be imported either via the web interface or the CLI using SCP or TFTP. In the web interface, select the **Device** tab and click the **Certificates** item on the left menu. Click the **Import** link in the **SSL Decryption Certificate** box and select the cert and key files and enter the passphrase for the certificate.



Certificate File: pan-ssl.crt

Key File: certkey

Pass Phrase: •••••

To do this via CLI, login to the device CLI and use one of the following commands:

```
scp import ssl-certificate from mike@10.0.0.43:/tmp/mycert.crt
```

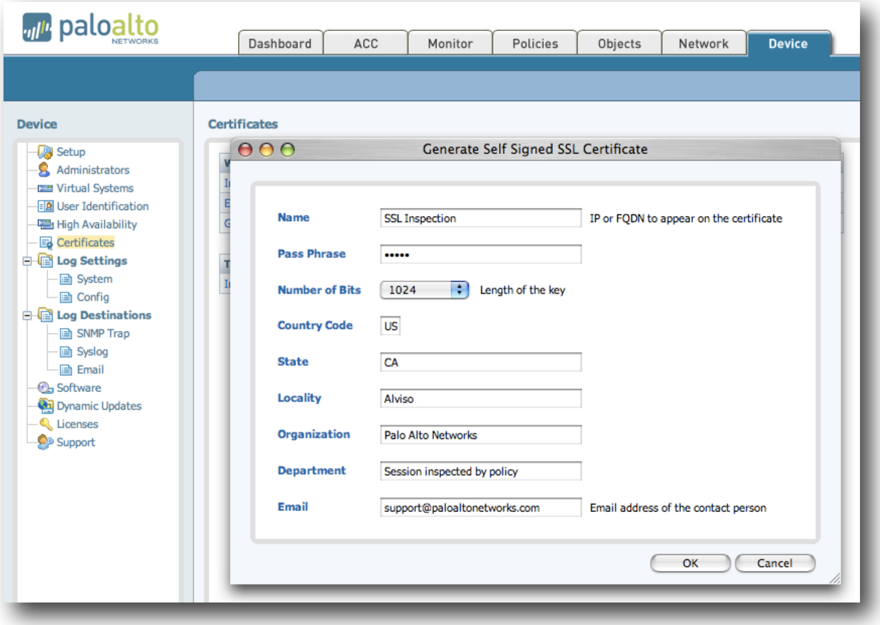
or

```
tftp import ssl-certificate from 10.0.0.43 file mycert.crt
```

For SCP, the source host must allow SSH connections. For TFTP, the source must be running a TFTP server.

Generating a New Self-Signed Certificate

If you do not want to load your own certificate into the device or use the default self-signed certificate, a new self-signed certificate can be generated via either the web interface or CLI. In the web interface, select the **Device** tab and click the **Certificates** item on the left menu. Click the **Generate a self-signed certificate** link in the **SSL Decryption Certificate** box and enter the desired details for the certificate. The details entered here are what users will see if they use browsers ability to view the CA certificate being used for an encrypted session.



Generate Self Signed SSL Certificate

Name: SSL Inspection — IP or FQDN to appear on the certificate

Pass Phrase: •••••

Number of Bits: 1024 — Length of the key

Country Code: US

State: CA

Locality: Alviso

Organization: Palo Alto Networks

Department: Session inspected by policy

Email: support@paloaltonetworks.com — Email address of the contact person

Use the following command on the device CLI to create a new self-signed certificate:

```
request certificate self-signed country-code US email support@paloaltonetworks.com locality
Alviso state CA organization “Palo Alto Networks” organization-unit “Session inspected by
policy” nbits 1024 name “SSL Inspection” passphrase bubba for-use-by ssl-decryption
```

Exporting the CA Certificate from the Device

The CA certificate can be exported either via the web interface or the CLI using SCP or TFTP. In the web interface, select the **Device** tab and click the **Certificates** item on the left menu. Click the **Export** link in the **SSL Decryption Certificate** box. The certificate will downloaded and saved by your browser.

To do this via CLI, login to the device CLI and use one of the following commands:

```
scp export trusted-ca-certificate to mike@10.0.0.68:/tmp
```

or

```
tftp export trusted-ca-certificate to 10.0.0.43
```

For SCP, the destination host must allow SSH connections. For TFTP, the destination must be running a TFTP server.

Considerations for High-Availability Deployments

When deploying a pair of devices in HA, each device needs to have a certificate installed to use for SSL decryption. As the certificates are not synchronized automatically, it is recommended to load the same certificate into both devices via the command above. Using self-signed certificates generated on each device is an option, but this will require both to be installed in the browsers so that the users will have a consistent experience regardless of which device is active.

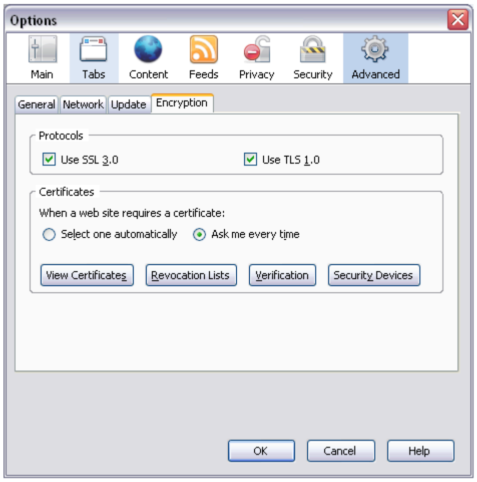
If an enterprise certificate is not available for loading into the device, a self-signed certificate can be generated using OpenSSL and loaded into each device.

Loading CA Certificates into Common Browsers

The following instructions cover the two most popular browsers, Internet Explorer 7.0 and Firefox version 2.0. Other browsers and versions of these browsers have very similar processes for loading trusted root certificates into the browser.

Firefox Version 2.0

1. Save public certificate to location that the computer can access it, such as the desktop, or a public folder on an Intranet server
2. Open browser
3. Select "Options" from Tools menu



Protocols

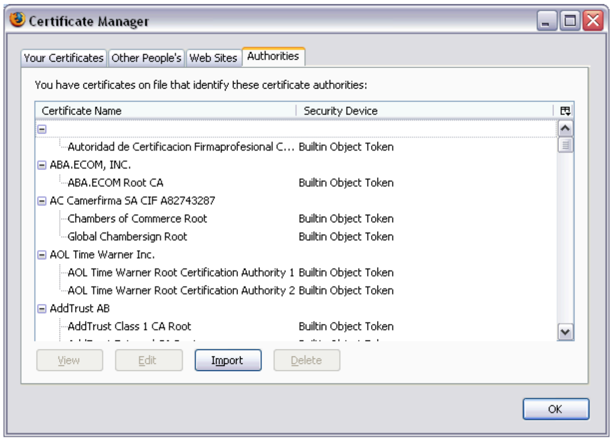
☑ Use SSL 3.0 ☑ Use TLS 1.0

Certificates

When a web site requires a certificate:

○ Select one automatically ● Ask me every time

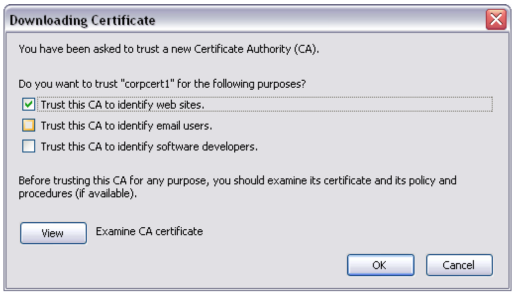
4. Select "Advanced", then "Encryption"
5. Select "View Certificates"



You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device
Autoridad de Certificacion Firmaprofesional C...	Builtin Object Token
ABA.ECOM, INC.	
ABA.ECOM Root CA	Builtin Object Token
AC Camerfirma SA CIF A82743287	
Chambers of Commerce Root	Builtin Object Token
Global Chambersign Root	Builtin Object Token
AOL Time Warner Inc.	
AOL Time Warner Root Certification Authority 1	Builtin Object Token
AOL Time Warner Root Certification Authority 2	Builtin Object Token
AddTrust AB	
AddTrust Class 1 CA Root	Builtin Object Token

6. Select "Authorities" from top menu bar
7. Select "Import" on bottom of menu screen
8. Browse to location of certificate and select certificate
9. Select "Trust this CA to identify web sites.



Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "corpcert1" for the following purposes?

☑ Trust this CA to identify web sites.
□ Trust this CA to identify email users.
□ Trust this CA to identify software developers.

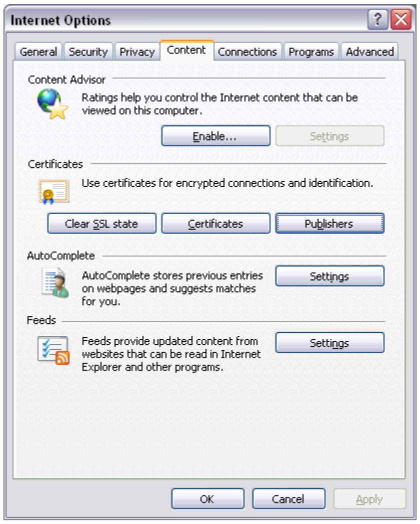
Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

View Examine CA certificate

10. Select "OK"

Internet Explorer Version 7.0

1. Save public certificate to location that the computer can access it, such as the desktop, or a public folder on an Intranet server
2. Open browser
3. Select "Internet Options" from Tools menu
4. Select the "Content" tab



Internet Options

Content Advisor

Ratings help you control the Internet content that can be viewed on this computer.

Certificates

Use certificates for encrypted connections and identification.

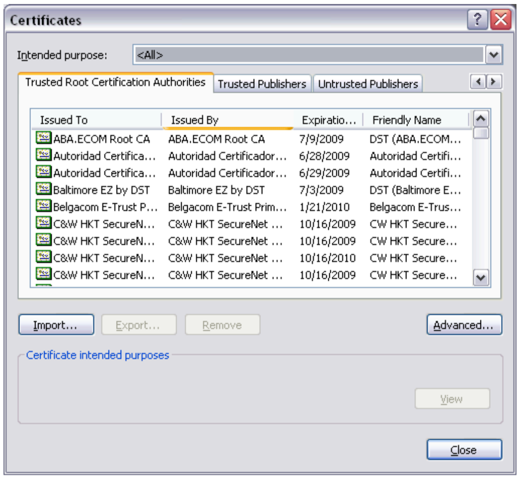
AutoComplete

AutoComplete stores previous entries on webpages and suggests matches for you.

Feeds

Feeds provide updated content from websites that can be read in Internet Explorer and other programs.

5. Select "Certificates" from Content menu
6. Select the "Trusted Root Certification Authorities" tab
7. Select "Import" from Certificates menu

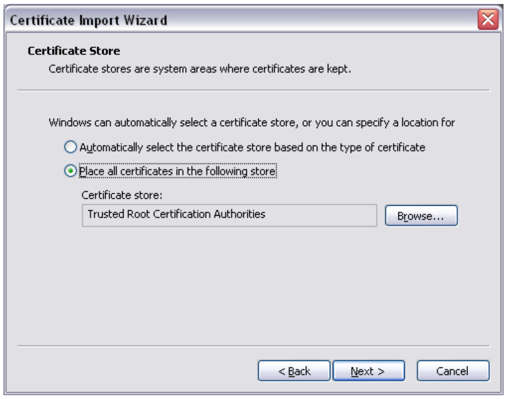


Certificates

Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
ABA.ECOM Root CA	ABA.ECOM Root CA	7/9/2009	DST (ABA.ECOM...
Autoridad Certifica...	Autoridad Certificador...	6/28/2009	Autoridad Certifi...
Autoridad Certifica...	Autoridad Certificador...	6/29/2009	Autoridad Certifi...
Baltimore EZ by DST	Baltimore EZ by DST	7/3/2009	DST (Baltimore E...
Belgacom E-Trust P...	Belgacom E-Trust Prim...	1/21/2010	Belgacom E-Trus...
C&W HKT SecureN...	C&W HKT SecureNet ...	10/16/2009	CW HKT Secure...
C&W HKT SecureN...	C&W HKT SecureNet ...	10/16/2009	CW HKT Secure...
C&W HKT SecureN...	C&W HKT SecureNet ...	10/16/2010	CW HKT Secure...
C&W HKT SecureN...	C&W HKT SecureNet ...	10/16/2009	CW HKT Secure...

8. Click Next
9. Browse to location of certificate and click Open
10. Click Next
11. Ensure "Place all certificates in the following store" indicates "Trusted Root Certification Authorities" as the certificate store



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

12. Click Finish and select "Yes" on the security warning asking if you want to install the certificate
13. Click Close
14. Restart Internet Explorer for the new certificate settings to take affect.

Adding to all Domain Computers via Active Directory

Using Active Directory you can add the SSL decryption certificate to the trusted roots in an Group Policy Object (GPO). To configure Group Policy in the Windows domain to distribute the SSL decryption certificate to the trusted root store of all domain computers:

1. Click **Start** -> **Programs** -> **Administrative Tools** -> **Active Directory Users and Computers**
2. In the left pane, locate the domain in which the policy you want to edit is applied.
3. Right-click the domain, and then click **Properties**.
4. Click the **Group Policy** tab.

5. Create a new **Group Policy** by clicking on **New** and give the new GPO a name
6. Click on the new object, and then click **Edit**. A new window opens.
7. In the left pane, expand the following items: 'Computer Configuration', 'Windows Settings', 'Security Settings', 'Public Key Policy'
8. Right-click **Trusted Root Certification Authorities**.
9. Select **All Tasks**, and then click **Import**.
10. Follow the instructions in the wizard to import the certificate.
11. Click **OK**.
12. Close the **Group Policy** window.
13. The certificate will now be loaded to all computers in the domain on the next group policy update. To update immediately, use the Windows **gpupdate** command.

Other Applications that use SSL

There are many applications that use SSL for communicating – including non-browser applications like email clients, collaboration tools, etc. Many do not check the CA certificate to ensure it is signed by a trusted CA. These applications should continue to work without modification. There are some applications that maintain a list of trusted CAs. In order for these applications to continue to function when performing SSL decryption, the SSL decryption certificate must be added to the applications list of trusted CAs. For instructions on how to do this, refer to the specific application's documentation. If it is not possible to add the certificate as a trusted CA certificate, the application should be excluded from being decrypted through a rule in the SSL Decryption Policy configuration.